Introducing a New Method Robust Against Crop Attack In Digital Image Watermarking Using Two-Step Sudoku

Mohammad Shahab Goli, M.S.c Student of
Optical Communication
Digital Processing and Machine Vision Research center,
Najafabad Branch, Islamic Azad University,
Najafabad, Iran.
Department of Electrical Engineering,
Najafabad Branch, Islamic Azad University,
Najafabad, Iran.
m.shahabgoli0015@yahoo.com

Alireza Naghsh, Assistant Professor
Digital Processing and Machine Vision Research center,
Najafabad Branch, Islamic Azad University,
Najafabad, Iran.
Department of Electrical Engineering,
Najafabad Branch, Islamic Azad University,
Najafabad, Iran.
Naghsh.a@pel.iaun.ac.ir

Abstract— **Several methods are exploited to watermark digital images as a safety measure for storing information, but an attacker can destroy the information by cropping a segment of the watermarked image. In recent years, numerous schemes were proposed that reduce the impact of such attacks. A new method has been proposed to confront cropping attack that is carried out using two sudoku tables. In this method, the watermark image is scattered in two sudoku table layouts with different solutions and is watermarked in the host image. Using this method, the watermark image is repeated 81 times in the host image, and to this effect the watermark image can be reconstructed using other segments when cropped by the attacker. Both sudokus used in this paper are in the classic 9x9 form and using this method, resistance to cropping attacks increases up to 98.8%.**

Keywords—component; cropping attack; digital image watermarking; spatial domain; sudoku.

I. INTRODUCTION

The internet, as a useful global communication system, plays an important role in data exchange. Due to the widespread of communication through virtual systems, quality and safety are two essential factors in data transmission. To increase safety level, one can make use of encryption and hiding. In the encryption method, if the key is exposed protection is no more guaranteed, therefore, data hiding, being more secure in this sense, is used [1].

Data hiding means to keep the important information out of reach and concealing them in low value data. Hiding is classified in two categories: steganography and watermarking. In steganography the message is visible but in watermarking the message can be both visible and invisible which is considered an important advantage [1].

In watermarking, the valuable information is embedded in worthless data thus guaranteeing their safety [2]. The information that is intended to be secured is called watermark information, the data in which the watermark information is concealed is called host data or host information, and the host data after embedding and watermarking is called watermarked information [3, 4]. The data or information can be in the form of text, video, audio and image [5].

Digital watermarking means putting the watermark information within the binary structure of the host data. If a picture is chosen to host the valuable data, it is called digital image watermarking [1]. Figure 1 illustrates a schematic view of information embedding in digital image watermarking.

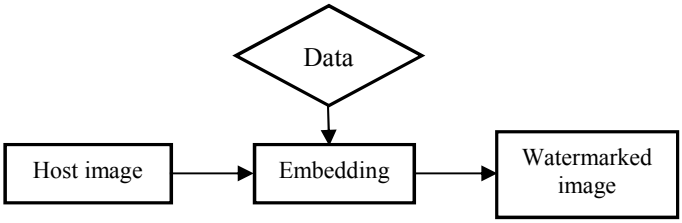

Fig. 1. A schematic view of data embedding in digital image watermarking [3, 4, 6]

Watermarking is categorized in spatial and transform domains. In the spatial domain, the watermark information is directly embedded in low value pixels of the host image. The most notable watermarking method in this domain is the Least Significant Bits (LSB). Two or three bits of valuable information is embedded in two or three low value bits of the host image. In transform domain, the watermark information is watermarked in the transformed form of the host image. the most important methods in this domain are Discrete Wavelet Transform (DWT), Discrete Cosine Transform (DCT) and Singular Value Decomposition (SVD) [1, 2].

The information needs to be extracted in the destination but it is prone to different attacks such as salt-and-pepper noise, compression, filter, cropping and etc. That damage the watermark information. The attacks mentioned in the spatial domain can harm the data, so in order to prevent this from

978-1-5090-6454-0/17/$31.00© IEEE

happening, instead of exploiting the methods in spatial domain, those of the transform domain are used. Figure 2 shows the framework of a typical watermarking system.

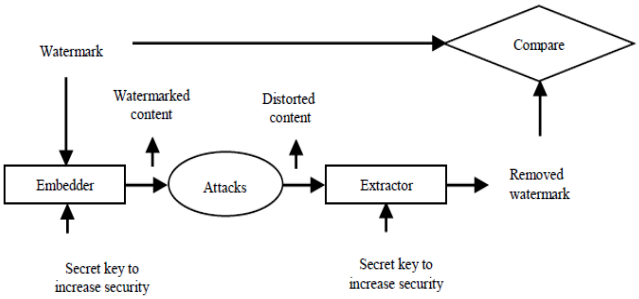

Fig. 2. Typical watermarking system framework [7]

A proper solution for the time spatial domain methods are used to watermark information in an image, is to have more than one copy of the watermark information in the host image. Hence, should one copy be damaged, it would be possible to reconstruct the data using the other pieces. This method is not resistant to cropping attacks, because the watermark information might not scatter well enough in the host image, thus making it impossible to extract the information from the copies in whole [8].

Another proposed method to confront cropping attacks is to use a sudoku table. In this method, the watermark image is organized according to a 9x9 sudoku table and is watermarked in the host image; Hence having 9 divided copies of the watermark image matching a sudoku solution and taking advantage from them to extract the information. In this fashion, resistance to cropping attacks is increased up to 94% [8].

A reasonable method to confront cropping attacks using two different sudoku tables with dissimilar solutions is proposed in this paper. This method that is based on using two classic 9x9 sudoku tables, offers more copies of the watermark image. This method provides 81 watermark images and increases the watermarking resistance up to 98.8%, significantly improving image watermarking resistance against cropping attacks compared to the other proposed methods in spatial domain.

In this paper, we present a new method for decrease effect of cropping attack in digital image watermarking. First of all, basic watermarking concepts such as attacks, application and requirements are introduced. Afterwards, gives an overview on outlining the problem, then introduces our proposed solution. In the last part, the results of the simulations is discussed

II. Defining the Basic Concepts

A. Cropping Attack

One of the attacks in spatial domain is cropping attack. It is when a segment of the watermarked image is cropped by the attacker thus harming part of the watermarked information. A reasonable method has been proposed in this paper to confront this kind of attack.

As you can see in table 1, maximum resistance to cropping attacks in recent studies, was between 50 to 94%. Cox et al. (1996), have proposed a transform domain watermarking system in which a signal scattered the watermark image all over the host image. In this method, the host image is needed to reconstruct the watermark image [9]. Fang et al. (2004), have proposed a blind watermarking method that had a 60% resistance to cropping attacks. This method was capable of watermarking 1kB of the watermark image but not resistant to arbitrary cropping attack [10]. Aggarwal and Singla (2011) made use of a greater amount of watermark information, but limited copies and inadequate locations resulted in a cropped image without the watermark information, when an arbitrary cropping attack occurred. This method was capable of watermarking 4kB of the watermark information in the host image, and 75% resistant to cropping attack, the host image was also needed when extracting the information [11]. Rawat and Raman (2010) were able to embed about 22kB of information but with a resistance not more than 50% to arbitrary cropping attack. This method needed the host image when extracting information [12]. Khalid et al. (2013) were able to watermark 28kB of watermark image with a 94% resistance to arbitrary cropping attack using a sudoku table solution [8].

Therefore, the current studies have resulted in 94% resistance to cropping attacks in digital image watermarking.

TABLE I. Comparing the resistant methods proposed in recent years

Schemes	Maximum Cropping Ratio Supported	Watermark Size
Cox et al(1996)	75%	Not fixed
Fang et al(2004)	50-60%	1 kB on one colour component
Rawat and Raman (2010)	50%	4 kB on one colour component
Aggarwal and Singla(2011)	75%	22 kB on one colour component
Ahmad khalid(2013)	94%	28 kB on one colour component

B. Sudoko

A sudoku table is composed of rows and columns that make up cells at their intersections, dividing the plane to N regions that have N cells each. A set of N numbers, called symbols, is placed in the cells. A classic sudoku is made up of numbers 1 to 9 filling the cells. In this type of Sudoku, the table is divided into 9 regions, each having 9 cells and in each cell a number (1 to 9) is put in a way that no number is repeated in any rows and columns and regions. Figure 3 shows a classic sudoku solution.

978-1-5090-6454-0/17/$31.00© IEEE

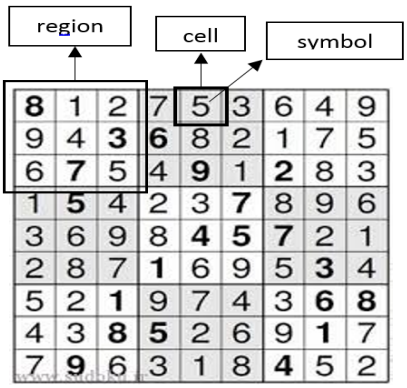

Fig. 3. An example of sodoku solution

The most significant advantage to a sudoku table is that every number is repeated 9 times in the table irregularly. There are 6.671×10^{21} different solutions to a classic 9×9 sudoku table[8].

C. Using The Sudoku On An Image

An adequate method for having multiple copies of the watermark image to confront attacks such as cropping or salt-and-pepper noise, is to use a sudoku table. In this method, first the watermark image is divided into 9 parts, as it is shown in figure 4.

Fig. 4. Dividing the watermark image to watermark it by a sodoku

Then, the divided watermark image is laid out to match a classic 9x9 sudoku. Figure 5 shows the baboon image laid out to match the sudoku from figure 3.

Fig. 5. The baboon image after applying the sodoku

Now if a cropping attack occurs, it would be possible to use other parts of the image to reconstruct it, since the baboon image is repeated 9 times in figure 5 [13-16].

III. Outlining The Problem

Watermarking by spatial domain methods have the advantages of simplicity, high speed and high capacity, but the main problem with this method is its low resistance to attacks such as cropping. Figure 6 shows an image that is watermarked in another using only LSB method with no particular scheme, then the water marked image was subjected to a cropping attack and finally the watermark image was extracted.

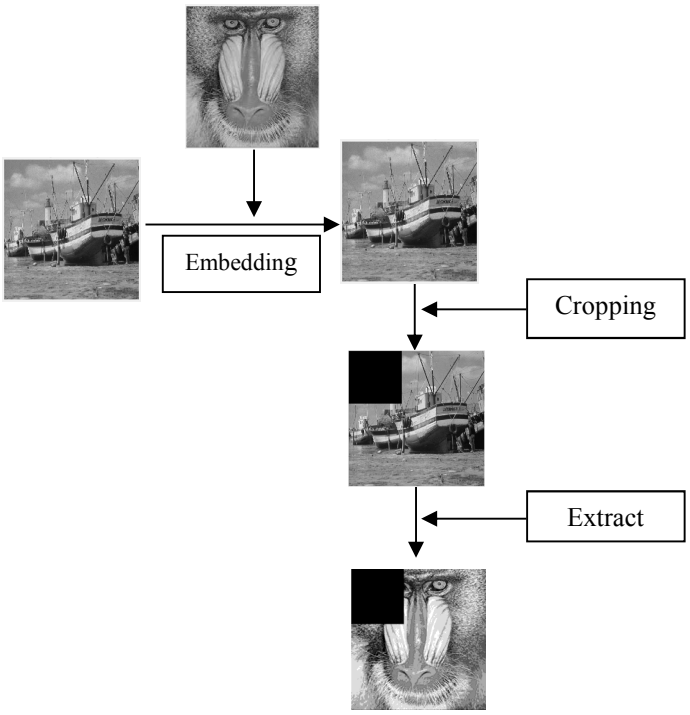

Fig. 6. 15.26% cropping attack on the watermarked image using the LSB

As you can see in the picture, any cropping attack on a watermarked image in the spatial domain, even in small percentages, damages the watermark information. Therefore, when using the spatial watermarking methods, suitable schemes are needed to be applied in order to keep the watermark information safe from harm should a cropping attack occur.

IV. The Proposed Solution

MATLAB standard pictures were used as the watermark and host images in this paper. The baboon picture is chosen to be the watermark image and the pepper to be the host image. Figure 7 illustrates the two.

a b

Fig. 7. a) Baboon picture (watermark image), b) pepper picture (host image)

Figure 8 shows the overall flowchart of the method used in this paper. In this research, it was intended to propose a new idea to improve the resistance of watermarking in spatial domain. Given the efficiency of the sudoku table in improving resistance, the existing studies have been aimed to exploit this method in

978-1-5090-6454-0/17/$31.00© IEEE

other ways. The reason for using the sudoku in watermarking is primarily increasing the number of segments that would be available. Secondly since the segments are scattered in the encrypted structure of the whole host image in a pre-defined layout, a better reconstruction of the watermark information would be possible after spatial attacks. In this regard, it was intended to propose a scheme that increases the number of watermark image segments, since having a greater number of these segments at hand strengthens the watermarking against higher percentage attacks, and more importantly to preserve the pre-encrypted structure of segments layout with a particular code. This would be quite helpful when reconstructing the information.

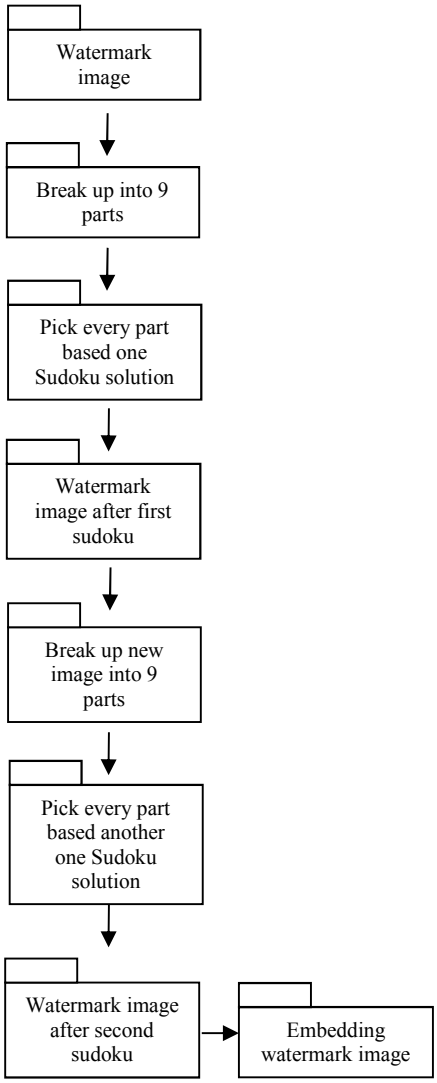

Fig. 8. The flowchart of applying sodoku on the watermark image in two steps wih two different sodoku solutions

A. First-Step Sudoku

In this step row and column dimensions of the baboon picture (watermark image) is determined with Eq. 1 and 2.

$$RS_{row}=m_c / m_w \cdot \sqrt{N} \quad (1)$$

$$RS_{coloumn}=m_c / m_w \cdot \sqrt{N} \quad (2)$$

Where, in the above equations m_c and n_c represent rows and columns of the host image respectively, m_w and n_w represent rows and columns of the watermark image and N is the number of segments. Then the watermark image size is changed with respect to the measured dimensions. Eq. 3 indicates the change in watermark image size based on the new dimensions calculated using Eq. 1 and 2.

$$w_t=resize(w_{org},RS_{row},RS_{coloumn}) \quad (3)$$

Where w_{org} is the watermark image in original size and w_t is the watermark image in new size. Then the resized watermarked image is divided into 9 segments, as in figure 4. In this step every segment is again divided into 9 and then the parts are laid out according to a sudoku solution and finally the 9 segments are set together. In this paper, the sudoku table shown in figure 3 was used at this step. Figure 9 shows the baboon picture after applying the first sudoku.

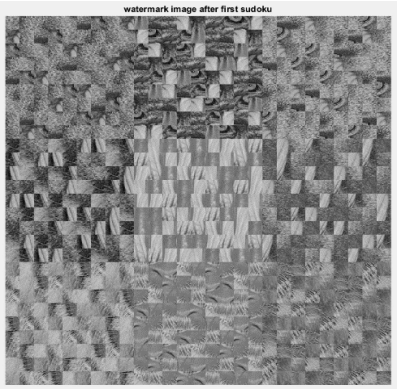

Fig. 9. The baboon picture after applying the first sodoku

B. Second-Step Sudoku

The watermark image that was obtained from applying the first-step sudoku in figure 9 is again divided into 9 segments as in figure 4, then laid out according to another sudoku. The sudoku table that was used here is shown in figure 10.

1	4	8	6	2	5	7	3	9
2	7	5	9	3	8	1	6	4
6	9	3	1	4	7	5	2	8
8	5	4	3	6	1	2	9	7
7	1	2	5	8	9	6	4	3
9	3	6	4	7	2	8	1	5
4	8	9	7	1	6	3	5	2
3	2	1	8	5	4	9	7	6
5	6	7	2	9	3	4	8	1

Fig. 10. The sodoku solution that was used in the second step of watermark image preparation

The baboon (watermark) image after applying the second-step sudoku is shown in figure 11.

978-1-5090-6454-0/17/$31.00© IEEE

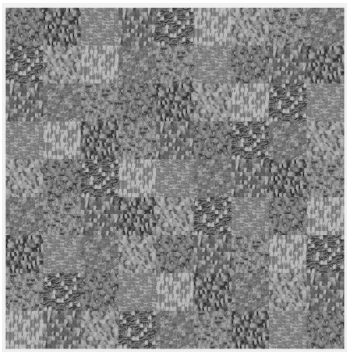

Fig. 11. The baboon image after applying the second-step sodoku

The image shown in figure 11 is the baboon picture that was laid out using two sudoku solutions with different codes in two steps. There are 6561 pieces of the original picture in this image that are laid out based on specific codes and are reconstructable. Now it is possible to watermark the baboon picture in other pictures using spatial methods, and be sure to a high extent that the information is safe against spatial attacks since if an attack occurs on the watermarked image damaging a portion of the watermark data, other parts of the image can be used to reconstruct the information. Figure 11 shows 81 copies of the baboon picture laid out using two sudoku solutions.

C. *Embedding the Watermark Image, Using the Least Significant Bits Method*

The most famous method of watermarking in spatial domain is the LSB. In this method, two or three valuable bits of the watermark image are embedded in two or three low value bits of the host image. Figure 12 shows how the watermark information is embedded in the host image using the method.

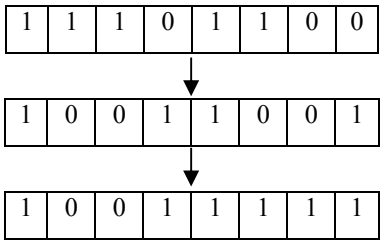

Fig. 12. Embedding three valuable bits of the watermark image in the host image using the LSB method

In this step, the baboon image of the figure 11 is embedded in the pepper picture using the LSB method. Figure 13 shows the result.

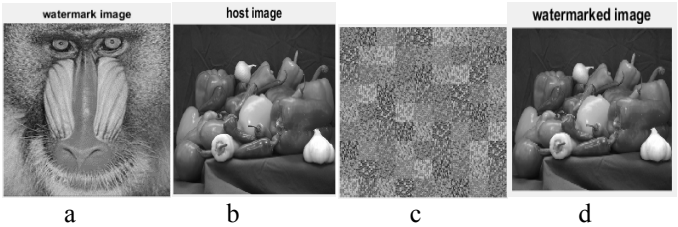

Fig. 13. a) The baboon picture (watermark image), b) the pepper picture (host image), c) the two-step sodoku applied on the baboon picture, d) the watermarked image

The watermark image can be extracted in the destination if the watermarked image is not attacked. Figure 14 shows the extracted watermark image before cropping attack.

Fig. 14. The extracted watermark image before cropping attack on the watermarked image

D. *Crop Attacking the Watermarked Image*

At this step, the watermarked image is crop attacked in different percentages. Figure 15 shows the watermarked picture of peppers crop attacked in different percentages.

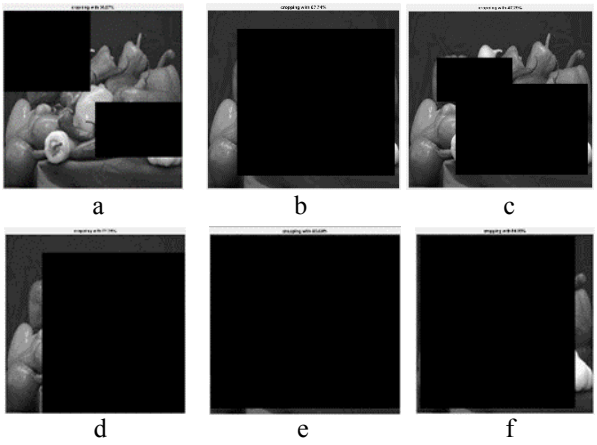

Fig. 15. Cropping attack in different percentages: a) 36.97%, b) 47.29%, c) 67.74%, d) 71.25%, e) 84.05%, f) 95.69%

After cropping attack the watermarked image up to the maximum percentage studied in this research, the extracted watermark image was the same as the image shown in figure 14. In other words, even after cropping 98.8% of the image, the extracted watermark image is the same one illustrated in figure 14.

V. CONCLUSION

Since there are many copies of the watermark image is embedded in the host image, using the two-step sudoku method, the resistance of the watermark information against attacks is increased up to 98.8%. In other words, the watermark image can be restored after cropping as much as 98.8% of the watermarked image, which is a significant progress compared to the existing methods. In addition to the baboon and pepper pictures, the watermarking was done using other standard pictures including lena and boat, which that are presented in table 2. The BER value between the watermark image and the extracted image using the LSB method is calculated in different cropping percentages and the results are presented in Figure 16. The watermark image was restored adequately up to 98.8% cropping and the BER value

978-1-5090-6454-0/17/$31.00© IEEE

was zero. The calculated BER values in figure 16 pertain to cropping more than 98.8% of the watermark image.

TABLE II. Comparing the PSNR of the results

Cover image	Watermark image	PSNR
Lena	Pepper	38.37
Pepper	Baboon	39.93
Boat	Lena	38.74
Baboon	Boat	39.60

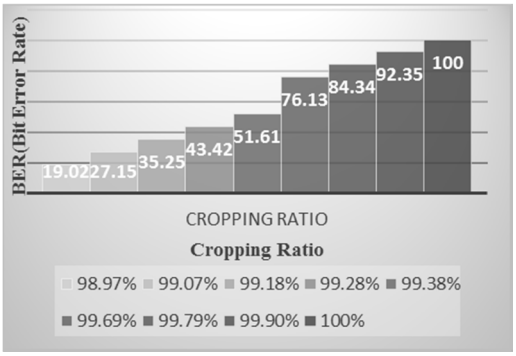

Fig. 16. The calculated BER diagram in different cropping percents

Although, watermarking using the spatial domain methods has the advantages of being fast, straightforward and high capacity, it is vulnerable to spatial domain attacks such as salt-and-pepper noise, compression and cropping. An adequate method for cropping attack resistant watermarking of digital images based on classic 9x9 sudoku table was proposed in this paper. Two different sudoku solutions were used in this method. Exploiting this method, it is possible to increase the resistance of watermarking by the LSB method of the spatial domain, up to 98.8% against cropping attacks. This method watermarks 81 repetitions of the watermark image in the host image, thus increasing the watermarking resistance against cropping attacks, in addition to keeping the advantages of the spatial domain watermarking. What's more, the method used in this research is a blind method and doesn't need the host image when extracting the watermark image, which is another advantage compared to the other existing methods. The BER value of the extracted image and the watermark image is zero until 98.8% of the picture is cropped, this means that a good image is extracted and there is no error in extraction even after cropping the image up to the mentioned percentage. The BER value increases with cropping percentage after that until 100% of the watermarked image is cropped, which means total data loss, and a 100% BER.

REFERENCES

[1] M.Mousavi, A.Naghsh, S.A.R.Abu-Bakar, "Watermarking techniques used in medical image:a survey," Journal of Digital Imaging. Volume 27, Issue 6, pp 714-729, 2014.

[2] Sunesh, H.Kumar, "Watermark attacks and applications in aatermarking", National Workshop-Cum-Conference on Recent Trends in Mathematics and Computing (RTMC) ,2011.

[3] D.Shukla, N.Tiwari "Survey on digital watermarking techniques," International journal of signal processing, Image processing and pattern, no.9 vol.8, 2016.

[4] M.Nangedda, R.A.Sudharsan, "Medical image steganography with digital watermarking", International journal advanced research in computer science and software engineering, volume 4,Issue 7,2014.

[5] Gupta, Vinita, Barve, Atul, "A Review on Image Watermarking and Its Techniques," International Journal of Advanced Research in Computer Science and Software Engineering,Volume 4, Issue 1, January 2014.

[6] M.Sh.Goli, A.Naghsh "A Comparative Study of Image-In-Image Steganography Using Three Methods of Least Significant Bit, Discrete Wavelet Transform and Singular Value Decomposition," Bulletin de la Société Royale des Sciences de Liège, Vol. 85, p. 1465 – 1474, 2016.

[7] Sh.Saneei, A.Naghsh "Introducing a new method of Robust Digital Image Watermarking against Cropping and Salt & Pepper Noise using Sudoku," Majlesi Journal of Multimedia Processing, Vol. 4, No. 4, December 2015.

[8] Sh.K.A.Khalid, M.Mat Deris, K.Malik Mohammad, "Anti Cropping Digital Image Watermarking using Sudoku," International Journal of Grid and Utility Computing Volume 4 Issue 2/3, 2013.

[9] Cox, I.J, Kilian.J, Leighton.T and Shamoon.T, "*A* Secure, Robust Watermark for Multimedia," Workshop on Information Hiding, University of Cambridge, 1996.

[10] Fang, Y.M, Huang, J.W and Wu, S.Q, "CDMA-based watermarking resisting to cropping," Proceedings of the ISCAS 2004**,** pp.25-28, 2004.

[11] Aggarwal.A and Singla.M, "Robust watermarking of color image under noise and cropping attack in spatial domain," International Journal of Computer Science and Information Technologies**,** Vol. 2, No. 5, pp.2036-2041, 2011.

[12] Rawat.S and Raman.B, "A new robust watermarking scheme for color images," Proceedings of the IEEE 2nd International Advance Computing Conference**,** pp.206-209, 2010.

[13] R.Shetty, B.R, Rohith.J, Mukund.V and Rohan, H., "Steganography using Sndoku Puzzle," in Proceedings of the IEEE International Conference on Advances in Recent Technologies in Communication and Computing**,** pp.623-626, 2009.

[14] Russell.E, Jarvis.F, "Mathematics of Sudoku 11," Mathematical Spectrum**,** Vol. 39, No. 2, pp .54-58, 2007.

[15] Wu, W.C, Ren.G.R., "A new approach to image authentication using chaotic map and Sudoku puzzle," Proceedngs of the IEEE 5th International Conference on Intelligent Information Hiding and Multimedia Signal Processing, pp.62843 1, 2009.

[16] Zou.Y, Tian.X.L, Xia, S.W. and Song, Y, "*A* novel image scrambling algorithm based on Sudoku puzzle, " Proceedings of the IEEE 4th International Congress on Image and Signal Processing**,** pp.737-740, 2011.

978-1-5090-6454-0/17/$31.00© IEEE